Simon v. Adzilla, Inc [New Media] et al Doc. 31

SEAN A. LINCOLN (State Bar No. 136387)
salincoln@orrick.com
I. NEEL CHATTERJEE (State Bar No. 173985)
nchatterjee@orrick.com
MONTE COOPER (State Bar No. 196746)
mcooper@orrick.com
THERESA A. SUTTON (State Bar No. 211857)
tsutton@orrick.com
YVONNE P. GREER (State Bar No. 214072)
ygreer@orrick.com
ORRICK, HERRINGTON & SUTCLIFFE LLP
1000 Marsh Road
Menlo Park, CA 94025
Telephone: 650-614-7400
Facsimile: 650-614-7401

Attorneys for Plaintiffs
THE FACEBOOK, INC. and MARK ZUCKERBERG

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

SAN JOSE DIVISION

THE FACEBOOK, INC. and MARK ZUCKERBERG,

Plaintiffs,

v.

CONNECTU, INC. (formerly known as CONNECTU, LLC), PACIFIC NORTHWEST SOFTWARE, INC., WINSTON WILLIAMS, WAYNE CHANG, and DAVID GUCWA,

Defendants.

Case No. 5:07-CV-01389-RS

PLAINTIFFS' REPLY IN SUPPORT OF MOTION FOR PARTIAL SUMMARY JUDGMENT RE DEFENDANTS' LIABILITY PURSUANT TO CALIFORNIA PENAL CODE SECTION 502(C) AND 15 U.S.C. § 7704(A)(1) AND 15 U.S.C. § 7704(B)(1)

Date: February 27, 2008
Time: 9:30 A.M.
Judge: Honorable Richard Seeborg

Dockets.Justia.com

TABLE OF CONTENTS

Page

I. INTRODUCTION 1
II. LEGAL DISCUSSION 1
  A. Summary Judgment Is Appropriate Under California Penal Code § 502(c) 1
    1. Plaintiffs Have Standing to Bring Claim Under California Penal Code § 502(c) 1
    2. Defendants' Access to Plaintiffs' Servers Was Unauthorized 2
    3. Plaintiffs Were Damaged Under Section 502(c) 3
    4. The Stolen Data Need Not Be "Private" 4
  B. Summary Judgment Is Appropriate Under the CAN-SPAM Act 5
    1. The Headers on Defendants' Commercial Email Were Materially False or Misleading 5
    2. Defendants Harvested Email Addresses in Violation of The Act 8
      a. Defendants "Harvested" Email Addresses in Violation of the Act 8
      b. Defendants Do Not Dispute that Their Attacks Were Knowing and Willful, Permitting Treble Damages 9
    3. Plaintiffs Have Standing 10
      a. Facebook Is an Internet Access Service 10
      b. Facebook Was Adversely Affected 11
  C. Defendants' Unclean Hands Defense is Unavailable 12
  D. Defendants' Request for Additional Discovery Should be Denied 14
III. CONCLUSION 15

TABLE OF AUTHORITIES

Page

FEDERAL CASES

Aitken, et al. v. *Comm'n Workers of America, et al*, 496 F. Supp. 2d 662 (E.D. Va. 2007) 6, 7

Chandris, Inc. v. *Latsis*, 515 U.S. 347 (1995) 3

Cortez v. Purolator Air Filtration Products Co., 23 Cal. 4th 163, 179-181 (2000)) 13

Copperweld Corp. v. Independence Tube Corp., 467 U.S. 752 (1984) 13

Facebook, Inc. v. *ConnectU LLC*, 489 F. Supp. 2d 1087 (N.D. Cal. 2007) 3, 10

Kiefer-Stewart Co. v. *Seagram & Sons*, 340 U.S. 211 (1951) 14

Leisnoi, Inc. v. *Stratman*, 154 F.3d 1062 (9th Cir.1998) 11

Mueller v. County of Los Angeles, 2008 U.S. App. LEXIS 615 (9th Cir., January 9, 2008) 15

Myspace, Inc. v. *Wallace*, 498 F. Supp. 2d 1293 (2007) 11

Omega World Travel, Inc. v. *Mummagraphics, Inc.*, 469 F.3d 348 (4th Cir. 2006) 7

Optinrealbig.com, LLC v. *Ironport Sys., Inc.*, 323 F. Supp. 2d 1037 (N.D. Cal. 2004) 11

PermaLife Mufflers, Inc. v. *International Parts Corp.*, 392 U.S. 134 (1964) 13

Phillips v. *Netblue*, 2006 U.S. Dist. LEXIS 92573 (N.D. Cal. 2006) 9, 10, 12

Pinter v. *Dahl*, 486 U.S. 622 (1988) 14

Roma Construction Co. v. *Arusso*, 96 F.3d 566 (1st Cir. 1996) 14

Tatum v. *City and County of San Francisco*, 441 F.3d 1090 (9th Cir. 2006) 14, 15

Thompson v. Sosa,

TABLE OF AUTHORITIES
(continued)

Page

2008 U.S. App. LEXIS 2141, 3 (9th Cir., January 14, 2008) 14, 15

U.S. v. *Shapiro*,
U.S. App. LEXIS 1468 (2nd Cir. 2002) 14

United States v. *Middleton*,
231 F.3d 1207 (9th Cir. 2000) 4

White Buffalo Ventures, LLC v. *University of Texas at Austin*,
420 F.3d 366 (5th Cir. 2005) 11

STATE CASES

Angelucci v. *Century Supper Club*,
41 Cal. 4th 160 (2007) 12

Gordon v. *Virtumundo*,
2007 WL. 1459395 (W.D. Wash. May 15, 2007) 10, 12

Hypertouch v. *Kennedy Western*,
2006 WL. 648688 (N.D.Cal. Mar.8, 2006) 11

Kofsky v. *Smart & Final Iris Co.*,
131 Cal. App. 2d 530 (1955) 13

Lass v. *Eliassen*,
94 Cal. App. 175 (1928), ... 12, 13

Estate of McInnis v. *Smith*,
182 Cal. App. 3d 949 (1986) 13

Myspace v. *TheGlobe.com*,
2007 WL. 1686966 (C.D. Cal. 2007) 6, 10

R.H. Dyck, Inc. v. *Haynes*,
2007 WL. 196755 (Cal. App. 3 Dist., Jan 26, 2007) 13

Timberline v. Jasinghani,
54 C.A.4th 1361, 1368 (1997) 13

Waters v. *San Dimas Ready Mix Concrete*,
222 Cal. App. 2d 380 (1964) 13

FEDERAL STATUTES

70 Fed. Reg. 12, 3115 (Jan. 19, 2005) 7

15 U.S.C. § 7701(a)(2) 12

15 U.S.C. § 7701(b)(2) 6

TABLE OF AUTHORITIES
(continued)

Page

15 U.S.C. § 7704(a)(1) 6

15 U.S.C. § 7704(b)(1) 8, 9, 12

15 U.S.C. § 7706(g)(3)(C) 9

47 U.S.C. § 231(e)(4) 10

18 U.S.C. § 1030(a)(5)(A) 4

Fed. R. Civ. P. 56(f) 14, 15

STATE STATUTES

Cal. Penal Code § 502(a) 3, 5

Cal. Penal Code § 502(a)(9) 3, 4

Cal. Penal Code § 502(c) 1, 3, 4

Cal. Penal Code § 502(e)(1) 2, 3, 4

I. **INTRODUCTION**

Defendants do not dispute a single material fact asserted by Plaintiffs Facebook, Inc. and Mark Zuckerberg in their Motion for Partial Summary Judgment. Instead, Defendants ask the Court to interpret various terms under the relevant statutes and deny Plaintiffs' Motion on the basis of their legal conclusions as to what those terms mean. Because Defendants' legal constructions are incorrect, summary judgment is appropriate. For instance, Defendants argue that resolution of this dispute turns on the legal significance of the terms "unauthorized" and "permission" under California Penal Code Section 502(c). Statutory construction does not raise a question of fact. Defendants do not dispute that they accessed Plaintiffs' servers for commercial reasons. Defendants simply claim they had permission from *Facebook users* to do so. As this Court has previously found, Plaintiffs must provide the requisite permission. Plaintiffs did not give Defendants such permission.

Defendants also do not dispute that Facebook was required to make modifications to its website security features to counteract Defendants' attacks. They merely challenge whether the modifications are the type of harm contemplated by Section 502 and the CAN-SPAM Act. Section 502(c) and the CAN-SPAM Act contemplate damage to include the cost of efforts made to assess any damage caused by those who hack into Plaintiffs' servers, including software features created to counteract Defendants' attacks to their systems.

Defendants do not dispute that the headers of the emails they sent to Facebook users were misleading or false. Defendants simply assert that they were not "materially" so, so as to violate the CAN-SPAM Act. The interpretation of this word is purely a legal issue. Under the law, Defendants' use of misleading and false headers was material. Defendants also challenge the language of the Act that confers standing on Plaintiffs, providers of Internet Access Services. Once again, this is a legal question. Summary judgment in favor of Plaintiffs is appropriate.

II. LEGAL DISCUSSION

A. Summary Judgment Is Appropriate Under California Penal Code § 502(c)

1. Plaintiffs Have Standing to Bring Claim Under California Penal Code § 502(c)

No factual dispute exists with respect to Plaintiffs' ownership of the Facebook "computer, computer system, computer network, computer program, or data" (hereinafter, "Computer System"). Cal. Penal Code § 502(e)(1). Defendants incorrectly argue that Plaintiffs have not shown that they "owned or leased" the Facebook website when the wrongful acts occurred. Opp'n 16:19-21. To the contrary, Plaintiffs introduced evidence establishing that they were, at all relevant times, the "owner[s] or lessee[s]" of the Computer System at issue. Declaration of Monte M.F. Cooper ("Cooper Decl."), Doc. No. 252, Exs. 1, 3-5, and 49.

For example, during his deposition, Zuckerberg testified that in order to launch the Facebook website in February 2004, he personally rented servers from managed.com. *Id.* Ex.1 at 84:15-85:25; *see also* Declaration of Theresa Sutton ("Sutton Decl.") Ex. A at 43:17-22. He was, therefore, the lessee and/or owner of the Computer System at issue at that time. Zuckerberg later executed computer data center agreements as an individual or on behalf of Facebook, Inc. in order to operate the website. Cooper Decl. Exs. 3-5. In March 2004, when the Savvy agreement was executed, no corporate entity existed or owned the site and, thus, Zuckerberg alone leased the server space and owned the equipment from which the website operated. Then, in the summer of 2004, new agreements were put in place to run the site that were signed on Thefacebook, Inc.'s behalf. *Id.* Exs. 4, 5; Sutton Decl. Ex. B. From that point forward, therefore, the Computer System necessarily was owned or leased by Facebook. Indeed, even Defendants' own selective evidence proves that at all relevant times Zuckerberg and/or Facebook owned or leased the Computer System. Declaration of Scott R. Mosko in Opp'n to Mot. for Partial Summ. J. ("Mosko Decl."), Doc. No. 294, Ex. A, 35:4-8; 242:12-25.

2. Defendants' Access to Plaintiffs' Servers Was Unauthorized

Defendants have not raised a fact issue as to whether they were authorized or received permission from Plaintiffs to enter the Facebook website and steal data. Instead, Defendants contend that the terms "unauthorized" and "permission" are undefined and, as a result, the Court must interpret these terms to determine who may provide the requisite authorization or permission. Opp'n 15:1-11. Defendants do not dispute that that their actions violated Facebook's Terms of Service, or that Plaintiffs never authorized Defendants to access the Facebook website to commercially harvest data. *See* Declaration of Mark E. Zuckerberg in Supp. Of Mot. for Partial Summ. J. ("Zuckerberg Decl."), Doc. No. 254, ¶ 10. Instead, Defendants argue that any registered Facebook user may authorize anyone else to access Plaintiffs' servers, take data from those computers (including data that the registered user did not itself put on the servers), and use the misappropriated data for commercial gain. The language and purpose of the statute demonstrate that Defendants' analysis is wrong, as does the evidence. Sutton Decl. Ex. I at 14:25:38-14:26:10. Moreover, Defendants offer no legal support for this proposition, and this Court already has rejected such an interpretation. *Facebook, Inc. v. ConnectU LLC,* 489 F. Supp. 2d 1087, 1091 (N.D. Cal. 2007). Section 502 was enacted to protect "individuals, businesses and governmental agencies from … unauthorized access to lawfully created computer data and computer systems." Cal. Penal Code § 502(a); Opp'n 14:22-24; Mot. 16:17-19. No reasonable interpretation of the statute could lead to the conclusion that anyone other than the owner or lessee of the Computer System may provide the requisite permission.

3. Plaintiffs Were Damaged Under Section 502(c)

Defendants incorrectly contend that the expression "damage or loss" in Section 502(e)(1) is undefined and, as a result, a factual issue exists as to whether Plaintiffs suffered any harm. Opp'n at 17. An interpretation of what constitutes "damage or loss" under Penal Code 502(c) is a legal question; it is not a factual issue. *See Chandris, Inc. v. Latsis*, 515 U.S. 347, 369 (1995) (holding that statutory interpretation is a question of law). Damage or loss should be interpreted broadly. The statute does not limit the types of damage or loss that can be suffered in any way, and defines a variety of harm. *See* Sections 502(a)(9), (10). Further, Section 502(e)(1) defines "compensatory damage" to include, without limitation, "any expenditure reasonably and necessarily incurred by the owner or lessee to verify that a computer system, computer network, computer program, or data was or was not altered, damaged, or deleted by the access." Cal. Penal

Code § 502(e)(1). Defendants argue that Plaintiffs have not been harmed for purposes of Section 502(c), because they claim the security measures Plaintiffs implemented were not in direct response to Defendants' attacks and the new features would have been implemented in any event. Opp'n at 17. Notably, Defendants are withdrawing the testimony of Winston Williams which forms the basis for this argument, and hence it now is unsupported. In addition, a computer hacking victim will be compensated for expenses associated with assessing potential damage to any system shown to have been improperly accessed. Cal. Penal Code § 502(e)(1).

Defendants erroneously rely on *United States v. Middleton*, 231 F.3d 1207, 1213 (9th Cir. 2000) and *In re Intuit Privacy Litigation,* 183 F. Supp. 2d 1272 (C.D. Cal. 2001), to suggest that damages based on the implementation of countermeasures, such as those at issue here, are improper. Opp'n 20:11-24; Shiflett Decl. (setting forth the various countermeasures developed in response to Defendants' attacks). *Middleton* and *Intuit* each interpret the term "damage" under the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030. The comparison in this context is not helpful. The particular CFAA section at issue in these two cases prohibited the transmission of code into a protected computer and intentionally causing damage directly to the computer. 18 U.S.C. § 1030(a)(5)(A). Section 502 is broader and expressly recognizes that there may be no actual harm caused to the Computer System beyond the unlawful intrusion. *See* Cal. Penal Code § 502(a)(9), (c), (e)(1).

In addition, the *Middleton* court held that "measures … reasonably necessary to resecure the data, program, system, or information from further damage" are reimbursable costs for purposes of assessing damages related to computer hacking. *Middleton*, at 1213. Here, Plaintiffs' countermeasures were reasonable and necessary to prevent Defendants' further intrusions into their systems.

Intuit is also completely inapposite insofar as that court analyzed whether the plaintiff was required to suffer economic damages in order to bring a Section 1030 claim. The court determined that economic damages were not required under the particular CFAA section. The claim ultimately was dismissed, however, because the plaintiff had not alleged that it suffered non-economic damages, and the complaint did not contain sufficient facts showing plaintiff satisfied the express requirement that economic damages, under CFAA, be at least $5,000. This analysis is wholly irrelevant to an interpretation of the term "damages" under Section 502(c).

4. The Stolen Data Need Not Be "Private"

Defendants contend once again that because Plaintiffs have not shown that the stolen data was private, they cannot prevail on summary judgment. Opp'n at 21:3-4. Nothing in the statute requires data to be private, as this Court already has expressly ruled, making the determination "law of the case." *Facebook, Inc.* at 1091 n5. The Legislature, in enacting Section 502, was concerned about the tampering, interference and integrity of computer systems and data. By prohibiting tampering and unauthorized access and safeguarding the integrity of data, the statute consequently protects the "privacy of individuals as well as [] the well-being of financial institutions, business concerns, governmental agencies and others … ." Cal. Penal Code § 502(a). The word "private" does not appear anywhere in Section 502(c), within the definition of "data," or within any definition related to the Computer Systems safeguarded by this statute. Privacy is simply not required for a finding of liability under Section 502(c), as this Court correctly ruled.

B. Summary Judgment Is Appropriate Under the CAN-SPAM Act

Facebook, an Internet Access Service, has been adversely affected by Defendants' sending its users commercial email messages that contained materially false or materially misleading header information.

Defendants do not challenge Facebook's evidence that the invitation messages Defendants sent to Facebook users qualify as commercial electronic mail messages (Mot. 19-20), nor do they challenge the evidence that Defendants initiated the transmission of such emails. Mot. 20-21. Defendants also do not dispute that Facebook suffered injury or that the messages contained false or misleading information. Instead, Defendants ask the Court to find that the injury suffered is not legally sufficient and that the information in the spam email headers was not *materially* false or misleading. These are questions of law, not fact. Summary judgment is appropriate.

1. The Headers on Defendants' Commercial Email Were *Materially* False or Misleading

Defendants argue that, although the header information on their spam emails to Facebook users was false and/or misleading, Facebook has not argued that the information was "**materially** misleading or false." Opp'n at 9. In their opening brief, Plaintiffs demonstrated that Defendants' use of false names (*e.g.*, god@harvard.edu or jstarr@[a variety of schools]) or names of third parties is "materially false or materially misleading" "because it is likely to affect the recipient's opinion of the value of the service advertised." *Aitken, et al. v. Comm'n Workers of America, et al*, 496 F. Supp. 2d 662 (E.D. Va. 2007). Defendants' contention to the contrary raises only a question of legal interpretation. Well-established law supports that the headers at issue were "materially" false and/or misleading.

Specifically, Section 7704(a)(1)(A) provides that:

> header information that is technically accurate but includes an originating electronic mail address, domain name, or Internet Protocol address the access to which for purposes of initiating the message was obtained by means of false or fraudulent pretenses or representations shall be considered materially misleading…

15 U.S.C. § 7704(a)(1)(A); *Myspace v. TheGlobe.com*, 2007 WL 1686966, at *5 (C.D. Cal. 2007) (emails found to be materially misleading because the "employees created fictitious email addresses and contact information . . . [and] Defendant failed to identity [sic] the messages as originating from TheGlobe.com"). Based on the plain language of the statute, Defendants violated Section 7704(a)(1) in two ways: by creating fake senders (*e.g.*, god@harvard.edu and jstarr@_______.edu)[1] and by "borrowing" accounts of already registered users. Notably, Defendants do not dispute that they created fake sender names to transmit spam email. Opp'n 11:3. Like the defendants in *Myspace, Inc. v. The Globe.com*, Defendants' use of fictitious email addresses "failed to identify the messages as originating from" www.connectu.com and, for that reason, violated the plain language of the Act. Defendants also do not dispute that they collected email addresses from the Facebook website using "borrowed" account information. Mot. 16:18-17:3; *see also* Sutton Decl. Exs. G, H. Having borrowed these accounts, Defendants concealed their true identity from Facebook while harvesting emails, which were thereby "obtained by means of false or fraudulent pretenses or representations." 15 U.S.C. § 7704(a)(1)(A).

Additionally, CAN-SPAM was designed, in part, to ensure "senders of commercial

[1] Defendants' Opposition does not address their creation of these fake sender accounts.

electronic mail [would] not mislead recipients as to the source or content of such mail." 15 U.S.C. § 7701(b)(2). The *Aitken* Court found headers forged with Verizon managers' names were materially misleading, in contravention of the Act's purpose, because the identity of the sender was likely to impact the effect of the spam email on the recipient. *Id. citing* 70 Fed.Reg. 12, 3115 (Jan. 19, 2005). *Aitken* and the present case are analogous.[2] Defendants attempt to neutralize the import of *Aitken* by relying on *Omega World Travel, Inc. v. Mummagraphics, Inc.*, 469 F.3d 348, 357-58 (4th Cir. 2006), a case that has no bearing on this matter. The *Omega* court found that the "inaccurate from line" was not materially misleading because each message offered other ways to identify the true sender, including an opt out hyperlink, a number to call for more information and a valid physical address. The spam at issue here contained none of these safeguards and, instead, demonstrates that the recipients actually were misled into believing the person named as the sender was the actually sender when, in fact, he was not. *See* Cooper Decl. Ex. 43. The fact that the spam emails contained a "hyperlink" to the website and were "replete with references to ConnectU" is of no import. An email actually forwarded by a friend who wanted the recipient to try out a new service or product also would include this information. This is precisely the type of deception the Act is designed to prevent.

Additionally, the Federal Trade Commission clarified the "materiality" requirement by noting the "test of whether a "from" line of an e-mail message runs afoul of CAN-SPAM entails resolution of two issues," including "[w]hether the 'from' line accurately identifies any person who initiated the message." Sutton Decl. Ex. C at 25431-32. The Commission noted that a "from" line does not contain sufficient information to respond to the actual sender if "a reasonable recipient would be confused by the "from" line identifier … ." The evidence also shows that the FTC recitation of the "materiality" test is met. Defendants do not dispute that Hannah Kim was confused by the "from" line identifier; indeed, her response (with a personal

[2] Defendants ask the Court to dismiss the "materiality" finding in *Aitken* because it was decided at the pleading stage. Opp'n 10:9-10. The timing of the decision is of no consequence to the determination that the headers were materially false or misleading. The *Aitken* court determined that, in light of the FTC's interpretation of "material," it could not conclude the misleading header information was immaterial. *Aitken*, at 667.

note) was meant for Thomas Cheng, the purported sender.[3] Instead, her response actually was received by webmaster@connectu.com. Cooper Decl. Ex. 43.

2. Defendants Harvested Email Addresses in Violation of The Act

a. Defendants "Harvested" Email Addresses in Violation of the Act

Defendants contend that they "did not harvest email addresses," while admitting they collected email addresses "via Social Butterfly." Opp'n 11:13-16; *cf*. Sutton Decl. Ex. I at 12:05:35-12:09:02; 14:13:06-14:21:25. The dispute is over the use of the word "harvest," not the legal standard. According to the Senate Committee, harvesting means obtaining email addresses "using an automatic address gathering program or process from a website or proprietary online service that has a policy of not sharing its user's emails for purposes of sending spam." Cooper Decl., Ex. 62 at 18. Social Butterfly meets this standard, as it comprises a series of computer "scripts" or programs that Defendants used to a) log in to the Facebook website; b) access data on its servers; c) collect or "grab" profile information, including email addresses; d) "crawl" or "spider" through the members' friends' profiles; e) collect or "grab" those friends' profile information, including email addresses; f) store that information in ConnectU's databases; and g) send spam email. Shiflett Decl. ¶¶ 10, 11. Defendants do not dispute that Social Butterfly (and its Importer/Crawler components) was designed precisely to collect email addresses automatically from the Facebook website. Thus, Defendants harvested email addresses from the Facebook website, where Facebook's Terms of Use forbid such activities.

Defendants also erroneously argue that in order for harvesting to violate the Act, the harvested emails must be used to send spam email. Opp'n 11:18-20. Section 7704(b)(1) prohibits the sending of spam *or* assisting in the collection of emails to which spam will be sent, where either event is preceded or accomplished by automated means. The phrase after "or" does not require the actual sending of spam email. Indeed, "the substance of § 7704(b)(1) deals

[3] "[T]he FTC reported that 42% of spam contains misleading subject lines that trick the recipient into thinking that the email sender has a personal or business relationship with the recipient. Moreover, email messages with deceptive subject lines may still lead unsuspecting consumers to websites promoting completely unrelated products or even scams."

completely with the improper procurement or creation of email addresses, which would be contained in a directory." *Phillips v. Netblue*, 2006 U.S. Dist. LEXIS 92573, at *9 n.1 (N.D. Cal. 2006). Defendants do not dispute that the "collection of emails" was accomplished by automated means or for the purpose of receiving spam email. Further, harvesting becomes violative when performed in contravention of a posted Notice indicating that user emails will not be sold or used for commercial purposes. 15 U.S.C. § 7704(b)(1)(A)(i). Plaintiffs, at all relevant times, posted the requisite Notice. Mot. 3:6-12; *see also* 2:20-3:6. Defendants' Opposition does not address the Privacy Notice.

b. Defendants Do Not Dispute that Their Attacks Were Knowing and Willful, Permitting Treble Damages

Defendants argue that they were not aware that their conduct violated the Act. Opp'n 12; Winklevoss Decl., ¶ 18. The "willful and knowing" element of Section 7706(g)(3)(C) is not concerned with ignorance of the law, but rather whether the spammer's harvesting and spamming activities were willful and knowing. *Phillips*, 2006 U.S. Dist. LEXIS 92573, *9-10 (aggravated damages available when violation involved "knowing and willful use of technology to facilitate" spamming). In fact, Defendants do not dispute that Social Butterfly and its component programs automatically collected email addresses from the Facebook website and used those addresses to spam Facebook users. Opp'n 11:13-16; Shiflett Decl. ¶ 10. Instead, Defendants challenge the competency of the evidence that demonstrates these violations. Opp'n 11:20-24; Plaintiffs' Opp'n to Evidentiary Objections, filed concurrently herewith. Such attacks raise only legal questions; they do not raise factual questions sufficient to defeat summary judgment.

Co-Defendant Wayne Chang's communications show that he and those with whom he communicated knew they were using Social Butterfly to access Facebook's server and "spider" through its user base to harvest email addresses and spam users. Mot. 22-23; Opp'n 12:24-13:4. Co-Defendant David Gucwa's instant messages to others, including defendants and their principals, demonstrate that Defendants "knowingly and willfully" used automated computer programs to scrape email addresses from Facebook's servers and send spam to Facebook users. Mot. 6-9; Opp'n 13:10-11. As a result, the Court has "discretion to increase (up to three times) the amount of statutory damages awarded if it finds" that the aggravated violations of 7704(b) involved "knowing and willful use of technology to facilitate acts in violation of other provisions of the Act." 15 U.S.C. § 7706(g)(3)(C)." *Phillips*, 2006 U.S. Dist. LEXIS 92573, *9-10.

3. Plaintiffs Have Standing

a. Facebook Is an Internet Access Service

Defendants once again raise the argument that they lost at the Motion to Dismiss stage – namely, that Plaintiffs are not as a matter of law providers of Internet Access Services for purposes of standing under CAN-SPAM.[4] This Court previously ruled in response to an identical argument that "ConnectU's contention that Facebook lacks standing to pursue this claim fails." *Facebook, Inc.*, 489 F. Supp. 2d at 1094.

Under Section 7702(11), "Internet access service" has the meaning given that term in 47 U.S.C. § 231(e)(4): "a service that enables users to access content, information, electronic mail, or other services offered over the Internet, and may also include access to proprietary content, information, and other services as part of a package of services offered to consumers." *Myspace, Inc. v. The Globe.com, Inc.*, 2007 WL 1686966, *3 (C.D. Cal.). As this Court already ruled, "the language [of 15 U.S.C. § 7702(11)] is broad enough to encompass entities such as Facebook that provide further access to content and communications between users for persons who may initially access the Internet through a conventional 'internet service provider.'" *Facebook, Inc.*, 489 F. Supp. 2d at 1094. Defendants do not dispute that Plaintiffs offer services over the Internet, including proprietary content, information and other services. *See* http://www.facebook.com. Moreover, both this Court and the *Myspace* court each rejected Defendants' position that only a traditional ISP has standing under the Act. *Id. See also Myspace, Inc.* at *4. A Facebook user's e-messages, like those on www.myspace.com, "reside[] at a unique URL, consisting of a string of characters that includes a reference to a user name or number, and the Internet destination, www.facebook.com." *Id.* at *4; Sutton Decl. Ex. D. Like the messages sent on MySpace,

[4] Defendants suggest that because Zuckerberg is "an individual" he lacks standing to bring a CAN-SPAM Act claim. Nothing in the Act, specifically Section 7706(g), indicates individuals lack standing. Prior to the incorporation of Facebook, Inc., Zuckerberg was the provider of the Internet Access Service known as www.thefacebook.com. He has standing to bring this claim. *See, e.g.*, *Gordon v. Virtumundo*, 2007 WL 1459395 (W.D. Wash. May 15, 2007).

Facebook messages fall under CAN-SPAM's definition of electronic mail, and Defendants have not presented any evidence to the contrary. *Id.*

Defendants also challenge the propriety of this Court's ruling that Plaintiffs have standing as an Internet Access Service under the Act. Opp'n 6:5-8. "The Ninth Circuit assumes that the legislative purpose of a statute is expressed by the ordinary meaning of the words used." *Myspace, Inc.*, at *3 citing *Leisnoi, Inc. v. Stratman*, 154 F.3d 1062, 1066 (9th Cir. 1998). "The plain meaning of the statutory language is unambiguous; Internet Access Service includes traditional Internet Service Providers, any email provider, and even most website owners." *Id.* citing *White Buffalo Ventures, LLC v. University of Texas at Austin*, 420 F.3d 366, 373 (5th Cir. 2005); *Hypertouch v. Kennedy Western*, 2006 WL 648688 at *3 (N.D.Cal. Mar.8, 2006). Under this broad definition, Plaintiffs are an "Internet Access Service," and the fact that this Court's finding that Plaintiffs qualify as an IAS occurred at the pleading stage does not diminish the fact that the finding is conclusive on this issue.

b. Facebook Was Adversely Affected

Defendants erroneously contend that Plaintiffs were not "adversely affected," or if they were, the harm was not significant enough to confer standing under the Act. Opp'n 6:17-23; 7:5-7. The interpretation of "adverse effect" is a legal question of statutory construction. Plaintiffs described in detail the substantial and measurable adverse effects they suffered as a result of Defendants' spamming activities. Mot. 12:12-14:25; 24:24-25:5; Shiflett Decl. Section D; Cooper Decl. Ex. 1 at 243:5-244:19; 248:5-250:13. *See also Myspace, Inc. v. Wallace*, 498 F. Supp. 2d 1293, 1305 (2007) (where court found plaintiff, having "incurred substantial costs in detecting, investigating, and remedying Defendant's unsolicited messages," issued a preliminary injunction). These facts are not questioned.

Plaintiffs also suffered harm to their business goodwill and reputation by sending messages to Facebook's userbase. Such harm is "unquantifiable and considered irreparable." *Wallace*, 498 F. Supp. 2d at 1305; *Optinrealbig.com, LLC v. Ironport Sys., Inc.*, 323 F. Supp. 2d 1037, 1050 (N.D. Cal. 2004) ("Damage to a business's goodwill is typically irreparable injury because it is difficult to calculate"). For a business whose main asset is its user base, attempts by others to steal that user base through spam poses a significant threat. Indeed, when contemplating CAN-SPAM, the Senate Committee recognized that an increase in spam could force consumers "to migrate" to other services. Cooper Decl. Ex. 62 at 6-7. Thus, the Committee specifically sought to "increase the privacy protection of consumers' e-mail addresses by outlawing the use of e-mail address collection methods." Cooper Decl. Ex. 62, at 13; 15 U.S.C. § 7704(b)(1). Though not every Facebook user spammed by ConnectU complained of the intrusion, some did. *See, e.g.,* Sutton Decl. Exs. E, F, H; *accord* Cooper Decl. Ex. 45. Courts have recognized they "cannot expect every user to complain about every piece of spam received, since users would spend as much time responding to spam as they would responding to non-spam messages." See 15 U.S.C. § 7701(a)(2) ("Unsolicited commercial electronic mail is currently estimated to account for over half of all electronic mail traffic . . .").

Defendants also erroneously contend that because Plaintiffs do not seek actual damages, but instead only statutory damages, they cannot show they were adversely affected. Opp'n 7:9-15. The statute allows for an election of damages based on the harm caused. *Phillips, Inc*., 2006 U.S. Dist. LEXIS 92573, *9-10. This choice also "indicates that Congress was more concerned with the spammer being appropriately punished than with the plaintiff being made whole." *Id.* Defendants improperly rely on *Gordon*, 2007 WL 1459395, to support this notion. In *Gordon*, the plaintiff admitted it suffered no harm whatsoever beyond having to sort through the spam email. *Id.* at *4. Unlike the plaintiff in *Gordon*, Plaintiffs have set forth evidence of various types of injury as a result of Defendants' hack and spam campaign. In *Gordon*, no election was viable because plaintiff said it was not harmed.

C. Defendants' Unclean Hands Defense is Unavailable

Defendants wrongly contend they can present an unclean hands defense. "[E]quitable principles may not be applied in opposition to statutory enactments." *Angelucci v. Century Supper Club*, 41 Cal. 4th 160, 179 (2007) (citing 13 Witkin, Summary of Cal. Law (10th ed. 2005) Equity, §3, p. 285); *see also Lass v. Eliassen*, 94 Cal. App. 175, 179 (1928) ("Rules of equity cannot be intruded in matters that are plain and fully covered by positive statute. . . . Nor will a court of equity ever lend its aid to accomplish by indirection what the law or its clearly defined policy forbids to be done directly"), cited in, *Timberline v. Jasinghani*, 54 C.A.4th 1361, 1368 (1997); *Estate of McInnis v. Smith*, 182 Cal.App.3d 949, 958 (1986) (refusing to apply principles of estoppel and equity in a probate proceeding because "the correct rule is that principles of equity cannot be used as a means to avoid the mandate of a statute"). Defendants attempt to distinguish *Lass* and *Timberline* by concluding that "[t]hose cases involved comprehensive statutory schemes governing probate and corporations respectively." Opp'n 24, 17-18. Nothing in the language of the decisions (one of which has remained undisturbed for eighty years) limits their holding to probate or some other statutory scheme. Defendants cite no support for their novel limitation that only select statutes are immune to unclean hands. Indeed, ample precedent to the contrary exists.

California courts have consistently and uniformly held that allowing the defense of unclean hands in any statutory context would be an unlawful circumvention of legislative intent, and thus void as against public policy. *See, e.g., Kofsky v. Smart & Final Iris Co.*, 131 Cal. App. 2d 530 (1955) (an antitrust case holding that "[i]t is settled that the equitable rule that 'he who comes into equity must come with clean hands,' has no application where the failure to restrain an act because the parties are in pari delicto would result in permitting an act declared by statute to be void or against public policy"); *Waters v. San Dimas Ready Mix Concrete*, 222 Cal.App.2d 380, 383 (1964) (application of the unclean hands doctrine in a case brought under the Labor Code would be unlawful and against public policy); *R.H. Dyck, Inc. v. Haynes*, 2007 Cal.App. Unpub. LEXIS 663, *22-*23 (Cal. App. 3 Dist., Jan 26, 2007) (rejecting defendant's contention that the plaintiff was a "corrupt corporate criminal" because "the unclean hands defense does not apply where its application would result in permitting or approving an act declared by law to be void or against public policy) (*citing Cortez v. Purolator Air Filtration Products Co.*, 23 Cal. 4th 163, 179-181 (2000)).

Notably, this policy is identical to that consistently espoused by the United States Supreme Court. *See, e.g., PermaLife Mufflers, Inc. v. International Parts Corp.*, 392 U.S. 134, 138 (1964), *overruled on other grounds by Copperweld Corp. v. Independence Tube Corp.*, 467 U.S. 752 (1984) ("We have often indicated the inappropriateness of invoking broad common-law barriers to relief where a private suit serves important public purposes . . . The plaintiff . . . may be no less morally reprehensible than the defendant, but the law encourages his suit to further the overriding public policy") (*citing, Kiefer-Stewart Co. v. Seagram & Sons*, 340 U.S. 211 (1951)); *Pinter v. Dahl*, 486 U.S. 622 (1988) (reaffirming that the *in pari delecto* defense "is not appropriate in litigation arising under federal regulatory statutes"); *see also, Roma Construction Co. v. Arusso*, 96 F.3d 566, 583 (1st Cir. 1996) (refusing to apply *in pari delicto* defense to a RICO violation). Another Circuit has underscored the obvious danger in allowing the unclean hands defense to apply in cases involving penal code violations. *See, e.g., U.S. v. Shapiro*, 2002 U.S. App. LEXIS 1468, *4 (2nd Cir. 2002) (holding that "It is no defense to a criminal charge to say that one's victim is also a criminal").

D. Defendants' Request for Additional Discovery Should be Denied

Defendants argue that Plaintiffs' motion for partial summary judgment should be denied on Federal Rule 56(f) grounds, claiming that "discovery necessary to defend against these claims is incomplete."[5] Opp'n 25, 11. Federal Rule 56(f) allows a court to grant a continuance on (or deny altogether) a motion for summary judgment when the party opposing the motion "shows by affidavit that, for specified reasons, it cannot present facts essential to justify its opposition." Fed. R. Civ. P. 56(f) (emphasis added). "A party requesting a continuance pursuant to Rule 56(f) must identify by affidavit the specific facts that further discovery would reveal, and explain why those facts would preclude summary judgment." *Tatum v. City and County of San Francisco*, 441 F.3d 1090, 1100 (9th Cir. 2006) (emphasis added) *cited by Thompson v. Sosa*, 2008 U.S. App. LEXIS 2141, *3 (9th Cir., January 14, 2008).

The only discovery Defendants contend is necessary to oppose Plaintiffs' Motion for Summary Judgment is a Facebook 30(b)(6) deposition "regarding the design of Facebook's servers used to operate its website, including information regarding bandwidth capability and network functionality." Opp'n 25:13-15. Defendants claim the deposition is necessary "to demonstrate that Plaintiffs were not adversely affected, as that term is used in the CAN-SPAM

---

[5] Defendants mischaracterize the facts leading up to the scheduling of Facebook's 30(b)(6) witness. *See* Sutton Decl. ¶ 10.

Act, by any of Defendants' alleged conduct because Plaintiffs' servers were not forced to suffer increased bandwidth or network functionality difficulties as a result of any of Defendants' alleged conduct in violation of CAN-SPAM." Opp'n 25:16-19. As discussed above, whether the type and amount of harm Facebook suffered is sufficient under the Act is a legal question and cannot be resolved by the introduction of additional facts. Further, whether Plaintiffs' "servers were … forced to suffer increased bandwidth or network functionality difficulties as a result of any of Defendants' conduct in violation of" the Act is irrelevant if other harm is shown, as it is here.

To the extent Defendants seek to rely on arguments made in their Rule 56(f) Motion (Doc. No. 259), the deficiencies in that motion were detailed in Plaintiffs' Opposition to Defendants' Civil L.R. 6-3 Motion For Order Enlarging Time To Oppose Plaintiffs' Motion For Partial Summary Judgment. Doc. No. 264. The discovery Defendants discuss in their original motion has nothing to do with their ability to oppose the current motion for partial summary judgment. Moreover, they failed entirely to comply with the requisite specificity for satisfying Rule 56(f). *See Tatum*, 441 F.3d 1090; *Thompson*, 2008 U.S. App. LEXIS 2141; *Mueller v. County of Los Angeles, 2008 U.S. App. LEXIS 615, *3 – *4 (9th Cir., January 9, 2008)*. Their request for additional discovery should be denied.

III. CONCLUSION

For the foregoing reasons, as well as those set forth in Plaintiffs' opening brief and supporting papers, summary judgment is appropriate.

Dated: February 13, 2008

ORRICK, HERRINGTON & SUTCLIFFE LLP

/s/ Theresa A. Sutton /s/

Theresa A. Sutton
Attorneys for Plaintiffs
THE FACEBOOK, INC. and MARK ZUCKERBERG

CERTIFICATE OF SERVICE

I hereby certify that this document(s) filed through the ECF system will be sent electronically to the registered participants as identified on the Notice of Electronic Filing (NEF) and paper copies will be sent to those indicated as non registered participants on February 13, 2008.

Dated: February 13, 2008.

Respectfully submitted,

/s/ Theresa A. Sutton /s/
Theresa A. Sutton